TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Annika Aavaste 163321IVCM

HOW TO IMPROVE DATA PROTECTION AND INFORMATION SECURITY IN LOCAL GOVERNMENTS USING GDPR COMPLIANT TRAINING

Master´s thesis

Supervisor: Eneken Tikk
PhD

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Annika Aavaste 163321IVCM

KUIDAS PARANDADA KOHALIKE OMAVALITSUSTE ANDME- NING INFOTURBE OLUKORDA ISIKUKAITSE ÜLDMÄÄRUSE ABIL LOODUD KOOLITUSEGA

magistritöö

Juhendaja: Eneken Tikk
PhD

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Annika Aavaste

13.05.2019

Abstract

In recent years, the Estonian government has contributed to make Estonia a well-functioning e-state. Although, the progress has been rapid and many tools and services are in use daily, the processing of personal data by local governments is still a major problem. The National Audit Office's 2018 audit highlighted a number of problems that continue to exist in local governments, despite the requirements of the General Data Protection Regulation that came into force as well as the national laws that have been in place for 10 years, regulating the security of personal data and information.

The National Audit Office found in its audit that the main problem is not acknowledging the risks of data processing in local governments. The officials are not aware of the real danger or the direct link between self-action/ inaction. Data is not considered as asset that needs protection. Nor are they aware of the requirements of the general regulation, in particular because they are not aware of the extent to which the general regulation applies to them and what requirements they should take into account.

The aim of this work is to analyse the results and weaknesses highlighted by the State Audit Office and to propose an improvement for the training course “Digitest” of the State Information System Agency. The outcome is a training module adapted to local government officials to cover the basic requirements of the general regulation and basic knowledge of personal data processing.

This thesis is written in English and is 59 -pages long, including 7 chapters and 8 figures.

Annotatsioon

KUIDAS PARANDADA KOHALIKE OMAVALITSUSTE ANDME- NING INFOTURBE OLUKORDA ISIKUKAITSE ÜLDMÄÄRUSE ABIL LOODUD KOOLITUSEGA

Viimastel aastatel on Eesti riik panustanud selleks, et muuta Eesti hästi toimivaks e-riigiks. Kuigi progress on olnud kiire ning paljud tööriistad ja teenused on igapäevaselt kasutuses, on siiski suureks probleemiks kohalikes omavalitsustes isikuandmete töötlemine. Riigikontrolli 2018. aasta audit tõi välja mitmed probleemid, mis eksisteerivad jätkuvalt kohalikes omavalitsustes, hoolimata nii kehtima hakanud Isikuandmete kaitse üldmäärusest tulenevatest reeglitest kui ka juba 10 aastat kehtinud siseriiklikud seadused, mis reguleerivad isikuandmete- ning info turvalisust.

Riigikontroll leidis oma auditis, et põhiliseks probleemiks on andmete töötlemisel tekkivate riskide mitteteadvustamine KOV-ides. Ei teadvustata reaalset ohtu ega seost otseselt enese tegevuse/tegevusetuse vahel. Andmeid ei peeta varaks, mis vajavad kaitset. Samuti ei teadvustata üldmäärusest tulenevaid nõudeid eelkõige seetõttu, et ei teata mil määral üldmäärus neile kohaldub ja millised on need nõuded millega nemad peaksid arvestama.

Käesoleva töö eesmärk on analüüsida riigikontrolli poolt välja toodud tulemusi ning nõrkusi ning nende põhjal pakkuda välja Riigi Infosüsteemi ameti koolituse „Digitest“ parendust, mis oleks kohalike omavalituste ametnikele sobivaks muudetud õppemoodul, mis kataks peamisi nõudeid üldmäärusest ning baasteadmisi isikuandmete töötlemisel.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 59 leheküljel, 7 peatükki ja 8 joonist.

List of abbreviations and terms

DPD	Data Protection Directive
EISA	Estonian Information Systems Authority
GDPR	General Data Protection Regulation
ISA	Information Security Awareness
KOV	Local Government
NAO	National Audit Office
NIST	National Institute of Standards and Technology
RIHA	Administration system for the state information system
X-ROAD	Estonian government secure data exchange platform

Table of Contents

List of figures

Introduction

For the last two decades the Estonian government's main emphasis has been on developing an efficient e-government. That has led to an awareness of the advantages of e-governance methods and a rapid growth of the technological solutions to provide them. Most of these solutions have been a great way for the citizen to connect and share data with the government without unnecessary waiting and bureaucracy. There are many success stories regarding Estonia becoming an e-country. In 2007, Estonia became the first country to allow online voting in a general election, which is one of a kind in the world. The possibility to communicate and convey documents between the citizen and the government without any physical connection and as with filing an annual tax return online, as 95% of Estonians do and which takes about 3 min [1]. Not to talk about digitally signing legally binding documents and the e-residency [2].

The vast evolution of e-governance and large amount of data processing in the public sector, has placed a burden to the local governments. Local governments are data processor in the meaning of General Data Protection Regulation (hereafter referred as the GDPR). Therefore they are obliged to protect the data of the citizens to provide privacy, availability and integrity.

Moreover, it can be said that many of the e-Government solutions face similar challenges as the e-businesses. As stated in the research paper by A. Conklin and G. White, that by adapting new technologies how the data is being delivered, stored or accessed, the mean of security have changed. Before adapting technology, the main emphasis was on the physical security, but when data is being moved between electronic channels, physical storage and security provisions and access control is significantly more complicated. To ensure the proper level of security, there should be a combination of managerial and technical executions. It is the obligation of the management to determine the level of risk tolerance and appropriate set of security requirements. [3]

According to the latest information cyber incidents have been increasing [4]. Many of these incidents or attacks may have serious consequences to either national security or for the personal data of the citizens. The protection of data and the vision of Estonia being the safest digitalized country is even mentioned in the new Cybersecurity strategy 2019-2022 [5] [6]. Moreover, in the new Information Security strategy for 2020, the aim is to improve the knowledge of the public sector [6]. Therefore, it is now more crucial than ever to protect the data of citizens from the very first point of contact with the government and GDPR provides the guidelines and requirements what needs to be met and NIST provides the theory on how to achieve it.

1.1 Purpose of the study

The GDPR regulates the relations between the data subject and the data processor. It also provides a tool for the data subject to take control of their data, when it comes to private sector.

Part of the problem with the local government and public sector institutions according to National Audit Office [7] is the lack of acknowledgement of threat in the public sector. The roots of this issue start from the management level. Combined with the lack of motivation, there are also issues with insufficient funding, in order to maintain all the infrastructure or a department of IT specialist.

Within the National Audit Office, the Information Security Authority made a statement, that there are plans to start educating the leading officials with the basics of cybersecurity. [7] But that may not have the full-scale impact needed. The leading officials may receive the proper trainings, but it is still uncertain that all of the knowledge will go forward to the official actually dealing with data processing every day.

1.2 Motivation of the study

As the author of the thesis is a student of Cybersecurity program in Tallinn University of Technology and has an interest in the data protection capabilities of local governments and the affects poor knowledge of data protection has on the data, information security and the development of information society, the author found it to be a challenging subject to research.

The outcome of this research is to provide a practical tool or knowledge, how to improve the data protection awareness trainings in local governments, by suggesting actual elaboration recommendations to an e-training planned to use to educate local governments officials.

1.3 Research questions

In order to achieve the objectives set by the thesis author, the questions of the research would be divided into main questions and supporting questions as follows:

1. What is the extent GDPR applies to local governments and does the local governments acknowledge the extent GDPR complies to them?

    - What impact the GDPR has on local governments and their data processing?

Under this question the author tries to determine the extent the GDPR applies to the local governments as data processors. What are the main articles and regulations applicable and what are the differences. In addition, the author tries to draw attention to the lack of understanding what the data withholds.

2. What are the means used in local governments to process data?

    - Who is responsible for the up keeping of the systems?

This question tries to shape the picture of the logic of the data processing means, in order to get an better understanding of the shortcomings made by the audits of Estonian officials.

3. What are the effects of poor knowledge of data processing has on the information security and development of information society?

    - In what way GDPR can be used as a safeguard or a tool to by the local governments?

    - How to elaborate the existing training and educational materials using GDPR as a tool?

This question analyses the effects poor data processing might have on the integrity, availability and confidentiality on the data and its overall impact to the information society and its development. In addition, the author suggest tools, derived from the regulations in order to improve the state of the situation.

1.4 Structure of the thesis

The structure of the thesis consists of the introduction which presents the subject, motive and the research questions, followed by the description of the research methodology, which will introduce the research methods used in the thesis.

The next part of the thesis, the author presents the main roles of the local governments in Estonia. In this chapter the author analyses the functions and commitments the local governments have. Followed by the chapter where the General Data Protection regulation is being analysed and compared with the functions and applicability and compliance with the tasks of the local governments.

It is then followed by the part where the author presents the technical structure and means used for the data processing in order to link and illustrate the issues presented by the official audits, perceived in the next chapter. In addition, the audit results are analysed to determine the effects it has on the development of information society and to information security.

Finally, the author presents the ideas on how to improve the situation of data protection in local governments by suggesting elaborations in a form of data protection module in the already existing “Digitest” composed by Information System Authority [8], using guidelines from the GDPR and NIST guide of trainings and many research materials, which provide the knowledge of what makes a successful awareness training.

Additionally, the last part of the thesis incorporates the description of the “Digitest” and a visual example of the suggested scenario for the local government module, followed by a summary, which suggest the ideas for following research, which is essential to validate the effectiveness of the training and the outcome it has on the information security in local governments.

1.5 Research Methodology

For this thesis the author will use the previously published materials- the audits performed by the officials, to analyse the most crucial shortcomings of information security in local governments and amongst the officials in order to suggest the best solutions for a module for an awareness training.

The methodology used for the data analysis is a document analysis and comparative analysis. As described by Bowen, the document analysis is a systematic procedure for reviewing or evaluating documents. There are many reasons to use document analysis as the research methods, because it provides background information, making it easier to understand the context. Additionally, it gives the possibility to understand more clearly the roots of the issues.

Document analysis involves skimming (superficial examination), reading (thorough examination), and interpretation. This iterative process combines elements of content analysis and thematic analysis. Content analysis is the process of organising information into categories related to the central questions of the research. [9]

The materials used for the analysations have been chosen due to their relevance for the topic. The documents are authentic, credible and accurate. The materials used are the results of the audits made by the National Audit Office, Data Protection inspectorate and Estonian Information System Authority, concerning the information security situation in the local governments.

The analyse is sectioned as follows: the first part is to analyse the documents related to the topic and then compare the results of the different audits, emphasising on the shortcomings from the audit which could be improved by a module in a training; Second part would be the analysis of the "Digitest" which is at the moment planned to be used to train the local government officials and will be followed by suggestions for improvement.

The "Digitest" has been chosen because information systems authority is the supervisory authority of local governments and their information security. Moreover, they have stated that the "Digitest" will be shared to local governments. [8]

The module for the local government officials will be created according to the National Institute of Standards and Technology published "Building an Information Technology

Security Awareness and Training Program" manual, which suggest the best practices in order to create a successful awareness training. [10] Additionally many other research materials on the matter are being analysed in order to provide the best solution for elaborating the awareness training environment.

2 Roles of local governments in Estonia

There is no elected regional government in Estonia, but a single-level local government. The representative body of a local government is the council, elected for four years by people permanently resident in the territory of the local authority. All local issues are managed and resolved autonomously by local authorities. [11] The council is responsible for the budget, taxes and accepting the statute and the development plan.

Local governments in Estonia have many commitments and functions in order to support the state. By the Local Government Organisation Act the main characteristics and the definition is that it is democratically formed legislative and executive bodies based on the division of the territory of the state into administrative units. [12] The main aim of the local governments is to decide and organize the local life, acting independently. [13]

Local governments in Estonia are carrying out the public administration tasks, which may be divided in to three tasks according to the content:

1. Voluntary local government tasks;
2. Mandatory constitutive tasks (i.e. tasks mandatory by law);
3. National tasks (enforced by law and under an administrative contract). [14]

2.1 Functions and competence of local governments

When taking into account that local governments are the institutions of democratic states, it is possible to define the core purposes of local governments. The core purposes can be derived from the "The European Charter of Local Self-Government (ECLSG)" [15] principles, which state that the local governments are the representatives of local communities and has the rights to decide and organize all the local aspects in the favour of the community. [14]

The functions of a local government include organising of social services and benefits and other social assistance, welfare services for the elderly, youth work, housing and

utilities, the supply of water and sewerage, the provision of public services and amenities, waste management, spatial planning, public transportation within the rural municipality or city and the construction and maintenance of roads and streets.

Also the function of organising childcare institutions, schools, libraries, health care institutions, shelters and care homes. [16]

As described above, the list of functions of a local governments is quite extent and many of these functions consist of data processing in many levels and much of which is of a sensitive nature.

3 General Data protection Regulation

The General Data Protection regulation came to force in 25th of May 2018. It proceeded the Data Protection Directive 95/46/EC (DPD) which was introduced in 1995. The Data Protection Directive (hereafter referred as the DPD) did not have as extensive reach and scope as the effective GDPR, the DPD was setting out aims and requirements for data protections standards comparing to GDPR, which is legally binding. Moreover, the GDPR brought new policies on consent, dealing with data breaches and penalties and compensations. [17]

The GDPR´s aim is to protect the natural persons in the relation to processing personal data as described in the Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). [18] Moreover, it should give individuals more control of their data, particularly when talking about use of technology when processing data, reducing administrative burden and unnecessary costs. Additionally, the aim is to cover all areas of data protection, making it comprehensive all around Europe.

Personal Data under the GDPR article 4, is defined as any information relating to an identified or identifiable natural person who is alive. In other words, information about a person whose identity is either manifestly clear or can at least be established by combining different sources of information that initially cannot identify an individual.

Considering that processing of personal data in the GDPR states that 'data processing' refers primarily to automated processing, but also to manual processing. Processing of personal data includes 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. [19]

The GDPR requires that systems and processes are compliant with "privacy by design", meaning that the privacy of the data collected is taken into account at all steps of the processes, it also requires that controllers discard personal data when it is no longer required. [20]

3.1 Main provisions derived from the GDPR and applicable for local governments

By the definition provided in the regulations article 4, the local government is an 'controller', which means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

And by the Article 6, the local governments process data according to:

Lawfulness of processing

1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*
2. *(e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
3. *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

As stated above, local governments are processing their data by the means of lawfulness processing. Many of the requirements on the data scope comes from different national regulations, although, many of them are now updated to be compliant with the GDPR. [21]

3.2 The main spheres and commitments the local governments have related to data processing

As the local governments have many assignments concerning the management of the life in local community, the data they are processing is covering many different types.

Local governments in Estonia have many commitments and functions as the data processors. The landscape of data collected in governments is defined by a range of sources including official records and statistics; secondary data obtained through administrative operations from front-end services. [22]

3.3 The main characteristics local governments have as data processors

Although, local governments are data processors, they are not processing persons data on the same basis as private sector. For public sector the rules on data processing differ. The public sector is either bound or obliged to collect and process data because of many different laws.

The GDPR determines the legal framework for rights and obligations of persons whose data are collected and processed (data subjects) and for companies and governments that collect and process these personal data (data controllers). [23]

3.3.1 Consent

Informed consent is believed to be an effective means of respecting individuals as autonomous decision makers with rights of self-determination, including rights to make choices, take or avoid risks, express preferences, and, perhaps most importantly, resist exploitation. Understood as a crucial mechanism for ensuring privacy, informed consent is a natural corollary of the idea that privacy means control over information about oneself. For some, these are the roots of privacy that must be respected in all environments and against all threats. [24]

The problem with data processing in local governments is, although informational self-determination can—theoretically—function effectively in private relationships, it functions poorly, and in many cases is not supposed to function, in citizen–government

relations. Citizens exercising control over what happens with their personal data, which is what informational self-determination involves, is at odds with the character of the public sector. First, consent cannot be an important ground for legitimising data processing by the government. Data processing in the public sector usually relies on legal obligations or a public interest; it would be difficult to maintain government records if they were compiled based on consent. Consent implies a choice between realistic options; citizens, however, cannot choose another government or different government services with friendlier privacy policies. Consent would only be meaningful if citizens could opt for a different form of social care with different forms of data processing—but that is not on offer. [25]

Therefore, the concept of consent does not apply for data processing in the local governments.

3.3.2 Erasure of data

First cases of "right to be forgotten" are well known [26] in the private sector, but in the public sector i.e. local governments versus citizens, this possibility is not as straight forward as expected. The regulations states:

Right to erasure ('right to be forgotten')

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;
(b)for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Data subject rights apply, in theory, to most governmental forms of data processing. However, this is limited to some basic standards of fair processing, such as having accurate and up-to-date data. Erasure might be requested, but depends on the government's determining whether it still needs the data. The rights do not involve any

form of control over how the data are processed for which purposes. So the government as data controller determines when, how, and why it processes data—citizens have nothing to choose here. Citizens do not determine which data the government can process in which ways, and there is no informational self-determination in the public sector. [25]

3.3.3 Transferring data

As stated above GDPR has some reservations when considering local governments and the data subjects right to transfer the data. Because the local government is processing data because of legitimate interest, which comes from a set of different laws, the data subject does not have the right to transfer data from one data controller to another. The exception in the data portability comes from the article 20, that states the data subjects right for data portability. In the article it is said that the data subject has the right to receive the personal data concerning him, which also applies, in the relationship between the data subject and the local government, and to transmit to another controller. This on the other hand does not apply when the processor is the local government:

The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Which means, that when the data is being processed by the official authority in the tasks carried out to performance public interest i.e. social assignments, childcare and so on.

However, even if the data subject cannot transfer the data to another controller, when talking about local governments and the data processed in them, the GDPR still requires that in any case of data transmission – this also applies to transferring data between local governments or other government institutions, there should be necessary security measures implemented:

(83)In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

As the NAO´s audit showed, many of the officials do not use secure ways i.e. encryption of data, when transmitting data. Which is an direct oversight of the regulation and is included in basic cyber hygiene knowledge.

4 The means used to process data in local governments

After regaining freedom, the technological development was fast. This led to a situation where Estonia is now considered as one of the most digitalized countries in the world. Our e-government solutions, i-elections[1] and the openness of the society is looked up to. The process of reforms and the direction in the evolvement of our government institution was to achieve the best possible e-government. Many of the decision of that time have been successful and Estonia has succeeded to achieve the fully functional e-government, where it is possible to arrange anything- from birth certificate, tax declaration or any other document which needs to be mediated between the citizen and the state. With the use of ID-card we can sign documents and to cast a vote, which is considered quite extraordinary. Estonia has even been called the most advanced digital society in the world. [27]

And in order to clarify the results of the audits, the thesis will provide an overview of the requirements local governments have considering when and how to process data and the technical means in use.

4.1 Estonian Data exchange: X-Road

From the Estonian Public Information Act chapter 5 [28] every public sector organisation or state organisation is required to keep an arranged collection of data used in the public sector about its citizens, according to valid legislation. All of these data collections need to be open and available for the public, unless stated otherwise i.e. sensitive data or other data which could harm a person when made public.

For a successful data transfer between different institutions and private companies, the state and most of Estonia's government supported sites and services are built on an X-Road data exchange service. It is an interoperable ecosystem and technical ability to exchange data, which allows different parties to exchange data between each other. In order to use the X-road, one must implement a security server and make the data exchange

[1] Internet voting (i-Voting or online voting) is a system that allows voters to take part in national or local elections by casting their ballots online via an Internet-connected computer, from anywhere in the world.

compatible with other X-road users. That all is made very easy by the fact that most of the codes used are public and reusable, making it easy for develop necessary solutions. [29]

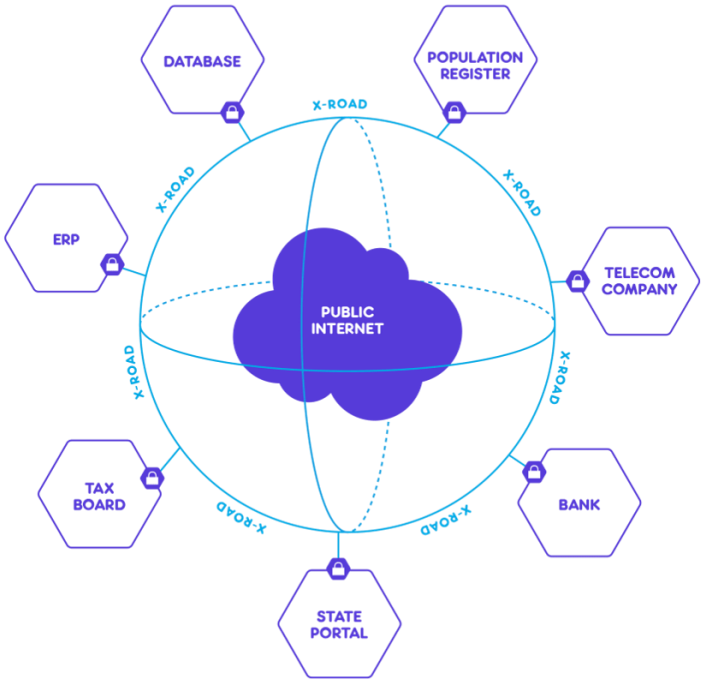

Figure 1. How does the X-road work (Source: EISA)

The aim with the X-Road was to make data exchange easy, available and secure – the data exchange over X-Road does not affect the integrity, availability or confidentiality of the data. [29]

4.2 Information systems and the administration system RIHA

The local governments requirement of collecting and organising data comes from the Estonian Public Information Act chapter 5^1 [28]. Another act which regulates the security and technical aspects of information systems is Information Security act [30] It defines the security measurements applicable for the local governments related to keeping an information system. These requirements have been mandatory for ten years.

Additionally, the local governments have the obligation to update the Administration system of the state´s information systems. The environment where the data collections and information systems are registered is an Administration system for the state information system (RIHA), which serves as a catalogue for the state´s information systems. [31]

RIHA gives information on the following:

- which are the information systems that make up the state's information system;
- which data are collected and processed and in which information systems;
- who are the information systems' owners, maintainers and contact persons;
- on which legal basis are the information systems operated and the data processed;
- the reusable components that ensure the interoperability of information systems (XML assets, classifications). [31]

The use of RIHA is regulated in the State Information System act, which determines the security features, the documentation for when establishing the information system and the inspection offices. [31] [32]

5 Affects the shortcomings in local governments data processing has on the information security and the development of information society

Throughout the year 2017 the National Audit Office performed an audit in ten local governments in order to determine the data protection and overall information security situation. [33] The results of the audit concluded that the conditions of data security are still not up to the standard for secure governance. The main issue being that the data collected and stored in local governments is still not secured as required and lot of the risks related to IT security is not highlighted enough.

Although, the state has contributed in the information security and to many different technical solutions, the problem lays in people and their mind-set. Moreover, the insufficient awareness of the direct consequences of the undoing or not acknowledging that data has value, depresses the development of information society.

All of the stated shortcomings are directly related to the state of information security and to the development of information society. When the officials lack of knowledge how to use the technology provided to them or have the fear of not succeeding using it, they most likely will avoid using it. [34]

5.1 Main issues of data processing in local governments related to GDPR

According to the audit carried out by the National Audit office, the most marginal issues that occurred in the local governments related to information security were, that the extent and the requirements of data processing is not acknowledged enough. As the requirements for processing data is derived from different laws, main activities and the possible results of consequences. Thus meaning, that the security necessities need to be defined and the security measures implemented. In many cases it was unclear for the officials, what is the value and requirements of security for different types of information, particularly when the official dealing with the types of data daily should be the best to determine the level of accessibility, confidentiality and integrity.

Moreover the NAO found that the audited local governments, do not fully understand the needs or the basics of the information security principles. They did not seem to realise the need for setting data security objectives or the need to register the information systems they are using to process data. These objectives are set in order to maintain the security of the data and every official should take these objectives into account when carrying out assignments. [33]

Another mistake NAO detected at least in two auditees out of ten was the processing of special categories of personal data (‘sensitive data’). When the sensitive data was transmitted between different recipients, the official did not implement any secure ways to do it. No measures were used, unless the recipient had not request it. Sensitive data was transmitted using open networks and no encryption used.

Similar results have been in the course of numerous audits done by the Estonian Data Protection Inspectorate [35] and the Estonian Information System Authority. [36] The issues local governments have been dealing with, have been pointed out for years. Already in the 2010 and 2012 the results of questionnaires proceeded in local governments show in the results, that the in 40 percent of local governments had trouble with the management of information technology and the situation does not support secure management of data.

EISA´s inquiries have shown through the years, that the local government officials and management does not find the information security subject relevant enough and the supervision and education from the state has been insufficient.

5.1.1 Recommendations according to the National Audit Office

As the result of the NAO´s audit, they made several recommendations to all parties in order to improve the information security. As the scope of this thesis is to focus on the deficits considering the compliance of GDPR. The recommendations which are related to GDPR were:

- To examine the need of requirements local governments have in information security and to examine why the compliance is not met.

- NAO´s suggestion for the EISA was to propagate more education programs to local governments and their officials. At this moment most of the trainings provided by ISA are directed more at the IT personnel.

- The need would be to educate the officials and EISA could develop an new concept of trainings. [37]

Therefore, when taking into account the recommendations of the NAO and the results of the audit, firstly there is a need to examine the root causes of why compliance is not met. What are the most important issues, that could also be incorporated into the awareness trainings scenarios, to address the official into properly acknowledging the mistakes and by suggesting the correct answers, increasing the awareness of correct behaviour.

Another suggestion for the EISA was to propagate more education programs to the officials without IT background or knowledge. Many studies indicate that managers with high information security awareness levels take significantly more and better actions to protect the organizational information assets. Additionally, on the institutional level, managers' awareness of information security as well as their support and commitment is suggested to have a positive influence on the employees' information security awareness levels. It is said the on the individual level, general knowledge of information systems, the type of education (e.g. technical vs. non-technical), as well as prior negative experience with information systems threats and incidents, could be the determinants of information security awareness. In order to avoid unintentional misbehaviour, practitioners should make an effort to improve the skills of employees who lack general information security knowledge, and further, should clearly communicate the damages the organization had to struggle with after prior policy violations and cyber-attacks, to make the personnel to be engaged and analyse the correlation between action and consequence. [38]

As for developing a new concept of trainings, suggestion would be a specifically tailored training model for local government officials. The local government module, which should consist of the scenarios relatable for the officials should be incorporated with the basic cyber hygiene module in order to provide a wide-ranging awareness.

Additionally, the procedure should not only consist of the training module, but also the training environment and the materials should be continuously improved and validated amongst the end users. That provides feedback for the creator of the training environment about the subjects and the aspects of data processing which have the biggest risk. That makes the evolvement of the awareness training up to date and the risks of threats lower.

6 GDPR as a tool to protect data in local governments

The GDPR could be used as a good collection of rules to implement into the data processing means. Moreover, when thinking about the numerous threats that have entered into force in recent years. For example there has been the Cambridge Analytica scandal and other incidents about misuse of personal digital data. These incidents have had the public increasingly aware of the kind of data is processed in many different situations. The digital fingerprints are ubiquitous, continuously generated, and processed with lightning speed. There is nearly limitless data-storage capacity, and data can be transferred, combined, and accessed from practically anywhere. [39] Making the possibilities of data leakages, misuse and breaches, defined as unauthorized access to defined categories of personal information, more frequent and the necessity to acknowledge that data is an essential asset.

As the governments are collecting citizens data in large amounts, it has led to an situation where there is a need to educate the educate a new generation of civil servants and to re-train existing workforce in embracing new technologies to ensure efficiency and continuity in the public sector. [22] Also the fact that interests and working practices of computing and policy domains typically tend to be very different, the trainings must be an requirement from a national level.

Because the actual protection, does not only depend on the legal framework, but also on the actual implementation and interpretation of the legislation and the ways in which it is enforced. The legislation on privacy and the protection of personal data contains many open norms that need further translation into workable, sector-specific, and context-specific rules and practices. [23] Additionally, all these practices should be implemented in the modern training possibilities – although, there are a wide range of information security awareness delivery methods such as contextual training and embedded training, in this case the best would be to use web-based training materials and an e-learning platform. [40]

Furthermore, the demand of education to raise the awareness of information security is also described in the DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high

common level of security of network and information systems across the Union, in chapter III Article 7:

1. Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information. The national strategy on the security of network and information systems shall address, in particular, the following issues:

(d)an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;

Therefore, the requirement of educating and awareness- raising is already stated in the regulation.

6.1 Improving awareness through training and using GDPR as a source of requirements

As stated in the Conklin and White paper, one possible method to test the knowledge and operational environments, is to use scenario based exercises. They say that an exercise to test a local government's ability to operate in a less than perfect cyber environment has provided insight into e-government operations and provided the participants an opportunity to determine their strengths and weaknesses. It allows to test the policies and procedures of the local government. [3] Although, information systems can be built to resist many different threats or attacks, they are still largely influenced by the actions of people. Therefore, the need for awareness trainings is essential to make people act in a certain way and security awareness efforts are seen as the "first line of defence". [41] Also surveys have shown that there are several mechanisms to help improve the end user behaviours from naive mistakes to better basic cyber hygiene, through awareness trainings. [42]

Therefore, the aim is to start training the government officials, as the learning process is an continuous procedure, the first step would be focusing on awareness training, which

then in the future builds into more elaborate and concentrated exercises and evolves into education, as described in the National Institute of Standards and Technology´s guide:

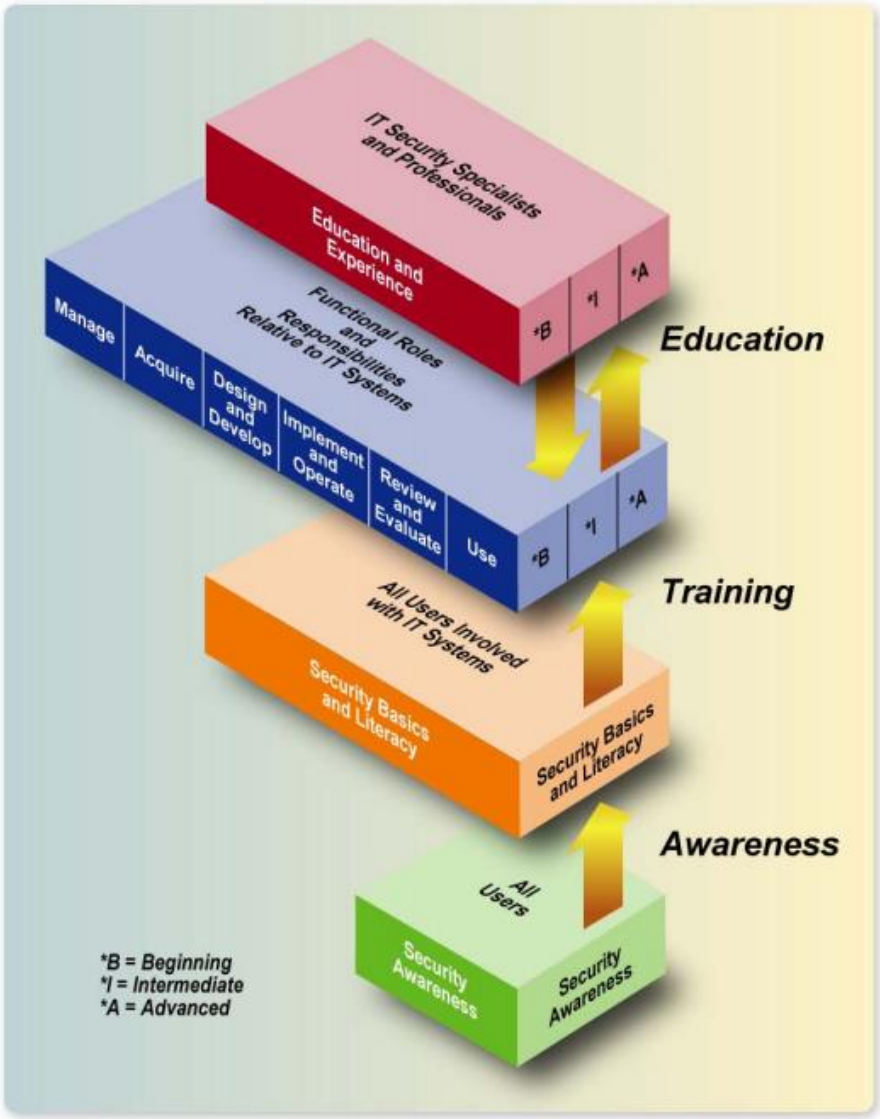

Figure 2. NIST IT Security Learning Continuum(Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf)

As stated in the National Institute of Standards and Technology´s guide, an IT security awareness and training program explains the proper rules of behaviours for the use of agency, or in this case local governments IT systems and information. The program should communicate IT security policies and procedures that need to be followed. It must precede and lay the basis for any sanctions imposed due to noncompliance. [10]

The NIST guidelines state that the security program which is successful should consist of IT security policy that reflects the needs of the organisation and the risks, which was missing from most of the local governments. Also, it should be constantly informed to the officials, what are their responsibilities related to IT security. The NIST directions state that: “Management should set the example for proper IT security behaviour within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers” [10]. Moreover, it is the foundation of a successful awareness training. And as brought out in the NAO audit, EISA should be more focused on the management level education instead of IT personal. A successful training explains the proper rules and policies of that institution and is consistent.

Additionally, when talking about Security awareness, the efforts are designed to change behaviour or reinforce good security practices. Awareness is defined in NIST Special Publication 800-16 as follows: “Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Therefore, when analysing the audits made by the officials, it is evident that in the local governments the first issue is the lack of awareness. It is the lack of acknowledgement about the security issues related to processing data and the way to improve that, is to build awareness. [10]

When it comes to awareness trainings, the programs must be designed with the organization mission in mind, therefore when dealing with data processing in local governments, it must be taken into account that local governments data processing differs from the data processing in private sector. It is important that the awareness and training program supports the needs of the organization and takes into account the needs of the institution. The most successful programs are those that users feel are relevant to the subject matter and issues presented. [10] Therefore, it is necessary to construct the training environment to comply with the needs of the officials and their need of knowledge about secure data processing and the information security basis.

And as described in the NAO´s audit recommendations, EISA should concentrate their trainings more on the non-technical level, keeping in mind the main aspects when building the awareness training for public officials need to incorporate the main themes derived from the GDPR and could be as follows:

- The means and requirements of secure data processing;
- The capability to define the different special types of data;
- The knowledge to implement different security measures according to the data type;
- Illustrations and examples of different scenarios in the case of data leakage or breaches.

Additionally, it is a fine line to determine whether the training is too complicated or too simple, it is most likely to be ineffective. Therefore, the best practice is not only to deploy awareness campaigns and educate users, but more related to the notion of the ability of users to understand risk and through that becoming more aware, which ultimately should be the objective and the structure of the "Digitest" supports. The audits showed that although, the requirements have been in force for a decade there are still inconsistencies in the deployment. The NAO suggested for EISA to determine the causes why, in spite of efforts to improve the situation, it is still not up to the standards.

Searches have shown that the obstacle of getting users to change their behaviour from using unsecure ways to insecure ways is down to many different factors. Among others is the factor of incompetence in the field of information security and the habit of using insecure ways. The audits have shown that the knowledge of information technology and security is on the lower level in the local governments [37], which is one of the causes why insecure ways are in use. Simply because the officials do not know, which are the best practices. Another research have proven information security awareness to be an essential direct and indirect determinant behaviour. For example, Galvez and Guzman (2009) identified information security awareness as one of the shaping factors of behaviour and consider that "… the higher the information security awareness, the higher the information security practice". [38]

It is stated that anyone who regards information in any form as an important asset, should be able to determine the possible threats related to it and the main perspective of carrying out awareness trainings, is to build the knowledge in the local governments, to be aware of the threats and avoid misconduct. [43]

In addition for awareness trainings, one option of eliminating use of insecure ways would just to force people to use secure ways. However, when enforcing stronger security measures, it in reality may cause more reluctance by officials to change their behaviour. In many cases, officials may view these security measures as impractical and a hindrance to their work. Without proper introduction and being unaware exactly what is required of them, may cause the officials to become reluctant to embrace these new security features. These inconsistencies in implementing policies among or within organisation's may lead to frustration by the officials and undermine the effectiveness of the policies. [41] Therefore, raising awareness before enhancing new and improved security measures, should have better results in providing security or to the understanding of the policies in place. Additionally, the aim of any awareness training is to improve the security practices of the trainees, not just to make them learn the guidelines but still unable to comply with them. [44]

In order to demonstrate the complexity of security behaviour and the compliance to policy is in fact made up of the intentions and attitudes of officials. This means that it is recommended to promote positive social pressure on officials with respect to compliance to security policies promotes actual security compliance. It suggest that the attitude of the officials against data security needs to be changed. Moreover, the attitude needs to be changed from the management level. [41] One of the NAO´s suggestions to EISA was to involve the management level to the training programs. [7]

Keeping that in mind the questions and scenarios should be as broad that the management level could also relate to. The suggested module of the course conforms with the "Digitest" and can be added to the modules, which include the cyber hygiene basics.

Moreover, the research made by T. Stephanou1 and R. Dagada [41] suggest the cycle and the outcomes of awareness training structure as follows:

First of all, the users will undergo security awareness training (1). Which will be in the form of security awareness material that will be exposed to users showing correct and

incorrect behaviours, but in the case of "Digitest" it also provides multiple choices to choose an answer, in order to later determine the risk factors for the trainee. The security message will be made explicit and disseminated to users (2). Explicit knowledge also needs to be made tacit by users internalising it. So, after the awareness material is presented, users will be required to write a short test that will measure to what extent the message has been internalised and in the case of "Digitest" it provides the input for creating the risk matrix (3).

Thereafter, the actual behaviour of respondents are measured to test whether their actual behaviour has changed due to awareness training (4) and, whether internalized knowledge (comprehension) is needed for appropriate behaviour (5).

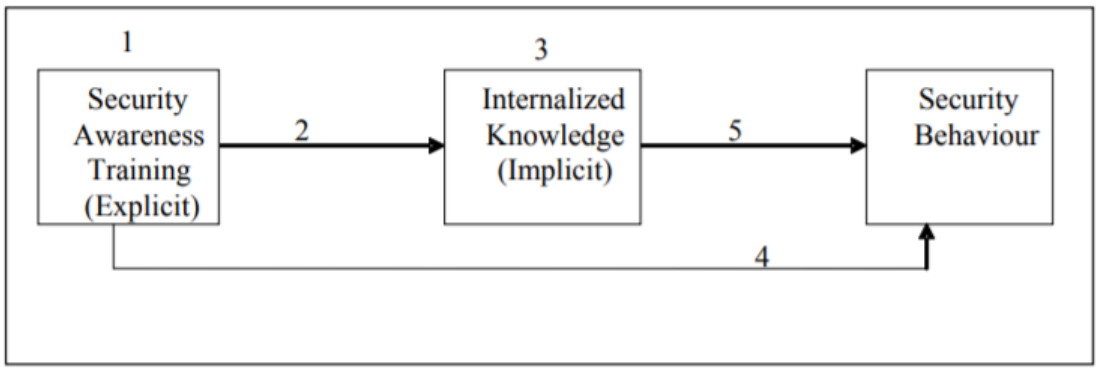

Figure 3. Theoretical model explaining how security awareness training affects behaviour. (Source: The impact of information security awareness training on information security behaviour: the case for further research)

An information security awareness program is considered effective if it can establish the appropriate knowledge and influence the attitude and behaviour of the participants towards positive changes in their security culture. To make sure that an awareness program has reached its objectives, appropriate measures need to be in place. The research conducted by Kruger and Kearney and described in the "A toolkit approach to information security awareness and education" research which suggests that changes in security behaviour can be monitored based on three dimensions: (1) what the employee knows (knowledge), (2) what the employee thinks (attitude) and (3) what the employee does (behaviour). Additionally. these dimensions were subdivided by them into further areas, for example the rules of keeping passwords and personal identification numbers secret, what are the ways of using the Internet and email in an appropriately safe manner and how to use mobile equipment carefully.

Moreover, to provide a complete insight of the effectiveness of awareness raising methods, that quantitative data should be combined with qualitative data for determining whether the desired effects have been achieved regarding user behaviour. Information security lies in the overlap of attitudes, knowledge, and behaviours. [45]

The structure of the "Digitest" supports the previously explained methods. It consists of the first part, which is an case or a scenario that determines what the official knows, what is the level of the knowledge, according to the answers it also provides an overview of the attitude the official has about information security, followed by multiple answers the trainee can choose from, providing the information of the officials actions in a similar situation (behaviour).

After the official chooses the answers, there will be a prompted explanation or study material of the correct answers and explaining the background and where possible suggesting tips which is the best way to act in a difficult situation.

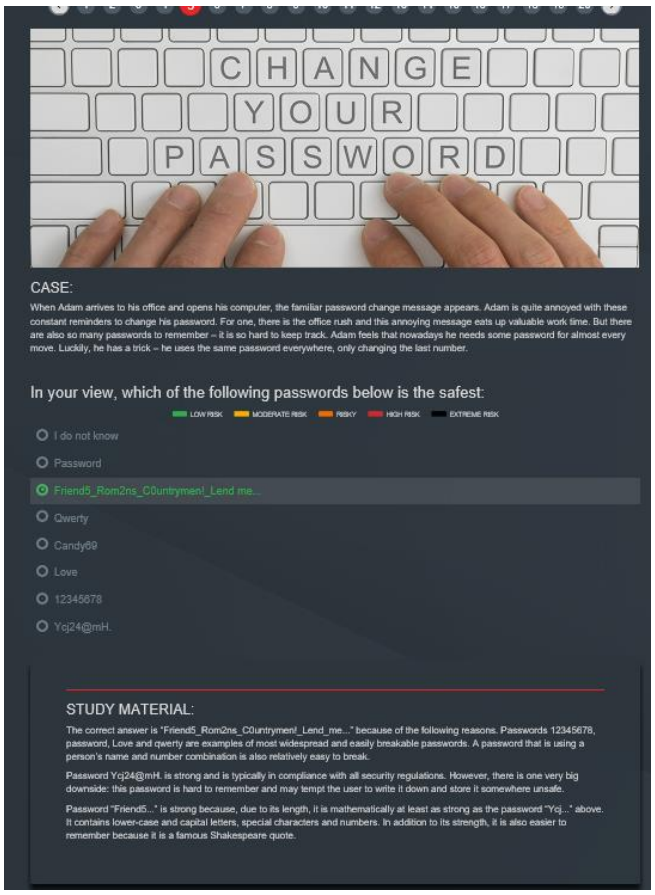

Figure 4. Print screen of EISA´s "Digitest" (Source: https://digitest.ria.ee)

After the study module is passed, the next section will be the test. The test is an indication of the level the study material was worked through, but does not present traditional “pass or fail” outcome.

This structure of the training environment is not meant to create a “pass or fail” situation, but to first address the risk behaviour [46] and by creating relatable situations, it makes the understanding of the threats and possible outcomes, more understandable for people without info technology background. Another aspect of this test is that it provides the users an overview of the threat vectors and risk areas, which are personally calculated and projected as a risk matrix.

Risk matrix generated of the answers the participants give throughout the course and the profile of the user is based on that same risk matrix which is also a foundation for the development of the course material and tests. The matrix is divided into four parts: personality, knowledge, exposure and belonging. That should not only focus on the technical aspects, but also to provide an overview of the risks related to the personality of the users. [46]

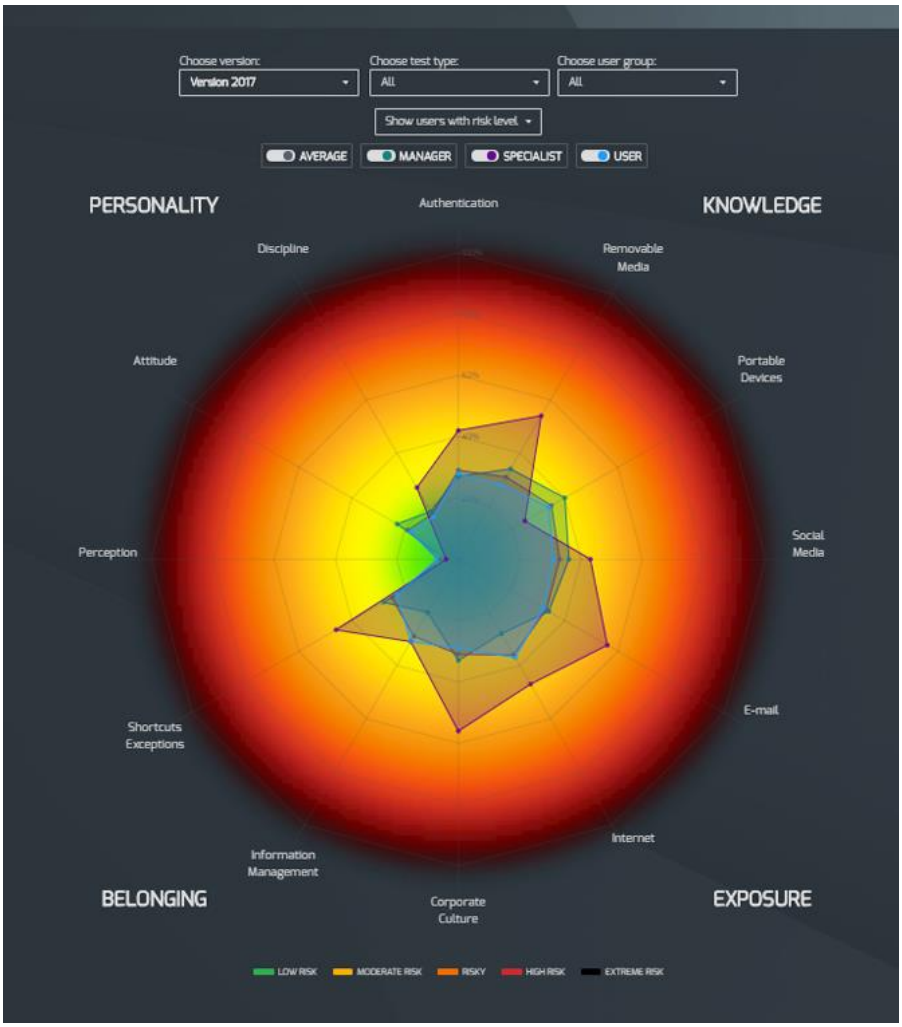

Figure 5. Example from the risk matrix (Source: Cybexer, https://cybexer.com/cyber-hygiene-e-learning-course/)

Following the structure of the test, the aim would be to provide a module, which mainly covers the GDPR and data protection, additionally with cases about the overall structure and scenarios which are common in the local governments. It would consist of scenarios, which are most commonly (according to the audit results) for been proven to be difficult for the officials. The aim is to get them to acknowledge the results, some actions might have, because research have shown, that misconducts may be a result to a very ordinary everyday action. As the audit results showed, many of the officials do not even acknowledge the threats coming from their own actions.

6.2 How to construct example scenarios

As the example used is “Digitest” the modules and test questions are created to match the structure of the same test. There will be presented a case, a question and the correct answer with a short description why the answer is correct. The main focus should help the official to eliminate possible misconducts with documents and information systems containing personal data.

Main aspects to focus when creating the questionnaires and cases, is to know the situations and procedures of the local governments officials in order to create situations, which they can relate to. As described in the previous paragraph, when the information provided is something the trainees can relate to, it is easier the remember the content of the training in the future.

The main themes the training should consist according to the results which came into light in the audits were:

- Description of the documents and data, how to determine the sensitivity:
- Transmit sensitive data in a secure way;
- How to determine the extent of GDPR- which data is considered personal data? Which data is considered as sensitive data according to GDPR?
- Sample scenarios to determine a possible threat situations to data – for the integrity, availability and confidentiality;
- To what extent the data should have restrictions? Should all documents be with restricted access.
- Who can access or inquire data? Is it only the data subject?

For example, the documents concerning the data about social care, school papers with the psychological analyse of the children, subsidies, data subjects health information could easily be determine to be sensitive data. With special categories or sensitive data, the cautions and appropriate safeguards for the rights and freedoms of data subjects, need to be applied in every aspect of the processing. This includes inserting the information to

information systems, transmitting the data either between government institutions or to the data subject, or when the data is being requested.

If the data consists personal data, the access to the data should be permitted in a way that only an official who has assignments related to that data, is permitted to access the data. Data should have desired level of protection to ensure the confidentiality referring, that only authorized parties can view the data, integrity refers that only authorized users are allowed to change the data and availability, referring to as resources being available when necessary. [3]

The safeguards in use need to prevent the accidental data leakages or breaches or harm in any other way for the data integrity, availability or confidentiality. The aim of the questions should be to make the official think and analyse the content of the data presented in the document and make a correct decision after that. By giving examples they can relate to, it makes the understanding of the GDPR requirement more comprehensive and therefore, the following action more thought through.

Most difficult part of creating a set of training questions, is to compose the scenarios, which the officials could relate to. This requires an insight to the daily assignments, possible situation that might occur or has occurred in the past and data, the official process on day to day basis. In order to get the best overview, one suggestion would be to involve local government officials into the creation process of the training scenarios. In order to incorporate accurate real life situations into scenarios, official from every department in the local government (social benefits, education, customer service representative etc.) should take part from information gathering action, either through semi-structured interview or workshop. Interaction provides the possibility to update and collect additional information directly from the source.

However, there is a risk of not getting entirely impartial answers using direct interviewing. Therefore, it is recommended to use the input from the authorities. For example another way of collecting the information of the main issues in local governments have, is to incorporate the inspectors of Estonian Data Protection Inspectorate [47] who have the obligation to arrange audits to the local governments and their data protection. It would be a source to determine the shortcomings they have noticed in data processing.

Additionally, EISA has the obligation to audit the local governments overall information technology situation, which should give them an overview of the shortcomings in that area. The overall outcome of the training environment would be to combine the modules into a comprehensive learning environment, where one part of the training would consist the basic cyber hygiene module and the module directed for the officials.

In order, to demonstrate the possible module for the local government officials there will be an added Appendix 1, which consists of scenarios that could be used. In the scenarios, the main focus is on the issues which were pointed out by the NAO and are related to GDPR. It is tried to tie the issues with relatable situations.

To demonstrate some of the scenarios and questions which could be implemented into the training environment and are presented in the Appendix 1, a web interface, with structure similar to EISA´s test, is added to this paragraph. It follows the structure stated above. The first part consists of the case- which provides the scenario or an situation description:

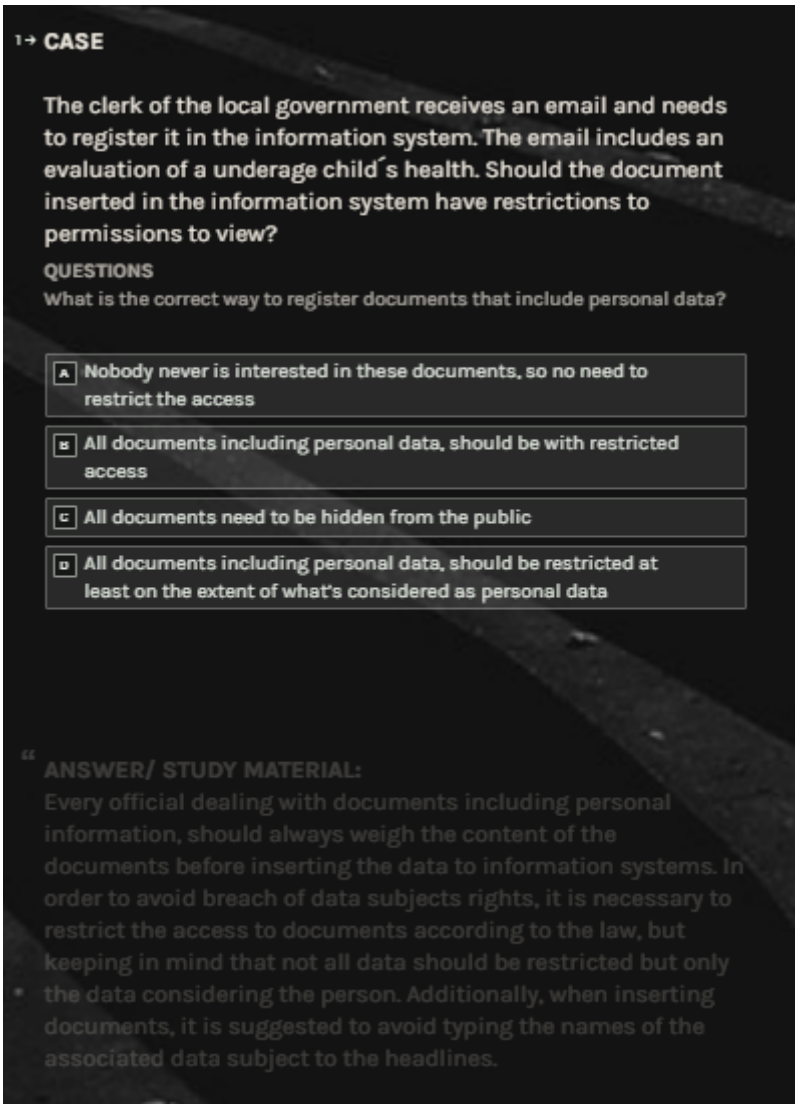

Figure 6. Example of created sample scenario and sample answers/study materials.

It is then followed by questions in an informal form and multiple choice answers, which are divided in a scale – low risk, moderate risk, risky, high risk, extreme risk. Dividing the answers according to risk allows the answers to add later be to a risk matrix, in order to determine the biggest shortcomings.

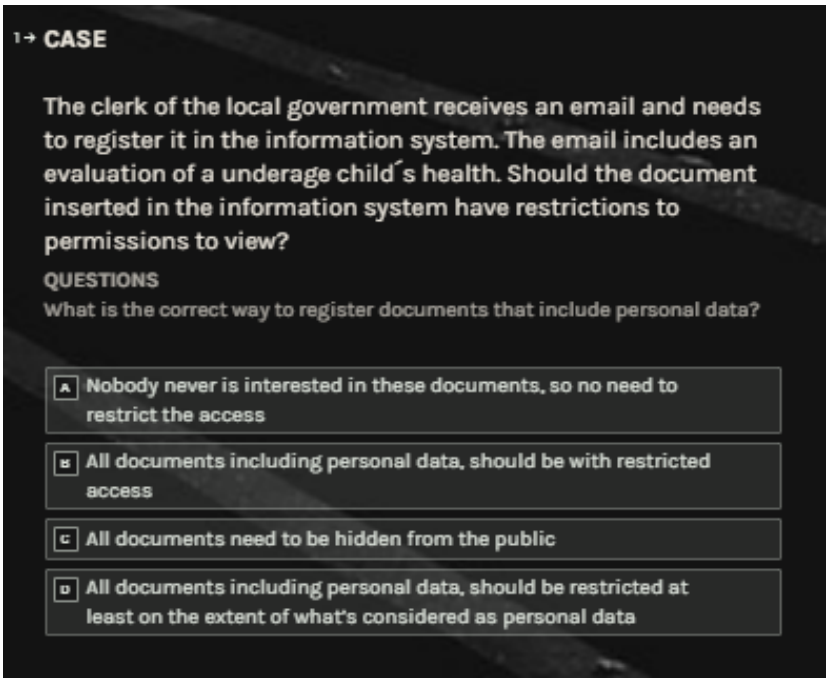

Figure 7. Example of a scenario and answer options

The multiple choice questions and answer are then followed by the study material. The Study material, as in the current cyber hygiene training, provides a brief explanation of the situation and the ways to act in similar situation:

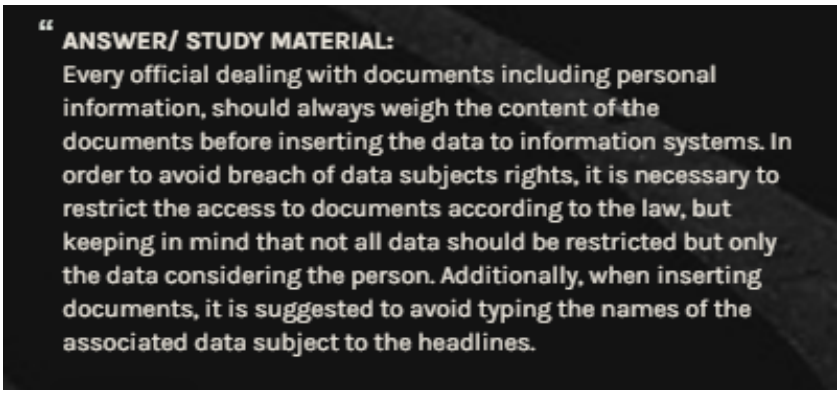

Figure 8. Example of the study material, providing the logical explanation

As in the “Digitest” this study material should also be followed by a test to get an indication of the results of how good has been the study material acquiring and according to the results, suggest ways to improve the areas which were the weakest and with the highest risk.

Additionally, it gives an overview of the overall situation for the composer of the training environment and the directions towards the parts that need more clarifying among the officials and the opportunity to update the test accordingly.

7 Summary

The development of technology and growth in the number of everyday users keeps on increasing, leading to a situation, where the state needs to keep up and adjust to the new ways of governing. Moreover, the governments and public sectors are expected to meet all sorts of different expectations- from the public and from other external factors, which may cause damage or harm to the sovereignty of the state.

As said in the introduction, many audits conducted, have concluded that the overall situation in local governments regarding data protection, is lacking the necessary security measures. Estonian local governments have the obligation to keep registered and arranged databases available for the public due to the Public Information Act paragraph 5^1 [28]. Moreover, not only the databases and the IT infrastructure should meet the security conditions presented in the General Data Protection Regulation, but also there is a need to educate and perform awareness trainings according to the regulation. [18]

The thesis first introduced the structure and the commitments local governments have in Estonia, additionally presenting the extent of the GDPR compliance to the data processing relations in between the data subject and the processor. Followed by an paragraph about the means used to collect and process data, in order to illustrate the full meaning of the audit results of National Audit Office, Estonian Information System Authority and Estonian Data Protection inspectorate.

The aim of the thesis was to analyse the audit results made by government institutions of National Audit Office, Information systems agency and the Data protection inspection. It was mandatory to first find out the most crucial shortcomings in order to suggest the module layout and subjects to be added to the e-learning environment.

Analysis showed, that the state of acknowledgement of information security is lacking in most of the local governments, starting from the management level. It was stated that the officials do not know how to determine the level of sensitivity of the data and a level of security it needs in order to achieve availability, integrity and confidentiality. Most alarming was the fact that special categories of personal data (‘sensitive data’) was transmitted without safeguards in use.

As suggested in the NAO´s audit, EISA should be more focused on the awareness trainings and education of the local governments officials including the management level. Therefore, the suggestion is to elaborate the existing "Digitest" with a module, which is directed mainly to educate the officials and their practices in data processing in order to achieve higher understanding of the threats data processing might endure. As stated above, the programs of awareness trainings must be designed with the organization mission in mind, therefore the e-learning modules should consist of problems or questions which the officials can relate to. However, the basic hygiene module should also be incorporated.

The materials analysed in this study indicated that the effectiveness of an awareness training comes from the subject matter represented in the training materials. Therefore, the materials need to be tailored to suit the officials operations, in order to provide subjects and scenarios that the officials could relate to. That enables the officials to fully comprehend the part they are representing in the information security functions and clarifying the rules and regulations.

7.1 Future work

As the research indicates, there is a need to increase the information security awareness among local governments official and to make them acknowledge their role in the process of ensuring the data protection. The aim of the research was to suggest a tailored module for the local government officials mainly concerning the issues, that they can relate to. Although, many research studies analysed in the course of this thesis, have showed that in order to achieve better results in the awareness trainings, the training must be built in a way that the trainee could relate to the subject and therefore is more engaged in the process.

However, in order to determine the effectiveness of the training materials and effects it has on the overall information security awareness, the future work should be validated through testing among sample audience. As the main focus was on creating suitable training environment for the local government officials the next step should be to continuously improve the environment.

In order to get some validation there should be a sample group or semi-structured interviews carried out with the end users from local governments, additionally, the sample group should consist of officials throughout the different departments in order to provide different aspects of data processing means. It is essential, that the end-user give feedback about the training environment and the materials it covers, in order to improve the scope, topicality and enhance the evolvement to a complete set of educational tool.

As the long term outcome would be not to only raise the awareness of information security but to build an educated security- aware society and government institutions, it is essential that the different parties keep a tightly connected cooperation.

References

[1] E. Zeynep ja P. Treleaven, „Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies,“ *The Computer Journal,* kd. Issue 3, pp. Pages 448-460, March 2019.

[2] „Republic of Estonia E-Residency,“ [Võrgumaterjal]. Available: https://e-resident.gov.ee/. [Kasutatud 11 April 2019].

[3] W. Conklin ja G. White, „e-Government and Cyber Security: The Role of Cyber Security Exercises,“ *Proceedings of the 39th Hawaii International Conference on System Sciences,* pp. 79b- 79b, 2006.

[4] „Information System Authority,“ 01 04 2019. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/2018-aastal-teatati-kuberjuhtumitest-kaks-korda-enam.html. [Kasutatud 16 april 2019].

[5] „Cyber Security Strategy 2019-2022,“ Ministry of Economic Affairs and Communications, [Võrgumaterjal]. Available: https://www.mkm.ee/en/objectives-activities/information-society/cyber-security. [Kasutatud 10 April 2019].

[6] „Digital Agenda 2020 for Estonia,“ Ministry of Economic Affairs and Communications, March 2019. [Võrgumaterjal]. Available: https://www.mkm.ee/en/objectives-activities/information-society. [Kasutatud April 2019].

[7] National Audit Office, „Implementation of system of IT security measures in local governments,“ 5 June 2018. [Võrgumaterjal]. Available: https://www.riigikontroll.ee/tabid/206/Audit/2466/language/en-US/Default.aspx. [Kasutatud 7 December 2018].

[8] „Ennetus ja nõuanded. Digitest,“ Estonian Information Systems Authority, January 2019. [Võrgumaterjal]. Available: https://www.ria.ee/et/kuberturvalisus/ennetus-ja-nouanded.html. [Kasutatud April 2019].

[9] G. A. Bowen, „Document Analysis as a Qualitative Research Method,“ *Qualitative Research Journal,* nr no. 2, pp. pp. 27-40, 2009.

[10] M. Wilson ja J. Hash, „Building an Information Technology Security Awareness and,“ 2003.

[11] K. Viks, „Europeanisation and transformation of public,“ *Berlin: Institut für,* p. Page 7, 2002.

[12] „Local Government Organisation Act,“ Riigikogu, Tallinn, 2016.

[13] „Local Government System in Estonia,“ Ministry of Finance, 12 April 2019. [Võrgumaterjal]. Available: https://www.rahandusministeerium.ee/en/local-governments-and-administrative-territorial-reform. [Kasutatud 12 April 2019].

[14] "Kohaliku omavalitsuse üksuste koostöö korraldulik raamistik ja võimelikud mudelid," Tallinna Tehnikaülikool Avaliku halduse instituut, Tallinn, 2012.

[15] Riigikogu, „Euroopa kohaliku omavalitsuse harta,“ Riigi Teataja, Tallinn, 1995.

[16] Riigikogu, „Functions and competence of local authority,“ Riigi Teataja, Tallinn, 1993.

[17] B. Piper, „What are the main differences between GDPR and the Data Protection Act?,“ *Virtual College,* January 2018.

[18] „REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,“ %1 *Official Journal of the European Union,* 2016.

[19] L. Floridi, Protection of Information and the Right to Privacy - a New Equilibrium?, Springer International Publishing, 2014, pp. 97-111.

[20] „The main differences between the DPD and the GDPR and how to address those moving forward,“ *British Legal Technology Forum,* 2017.

[21] Riigikogu, „Isikuandmete kaitse seaduse rakendamise seadus,“ 2018. [Võrgumaterjal].Available: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/778XIII_Isiku_rak_s_2019.pdf. [Kasutatud April 2019].

[22] Z. Engin ja P. Treleaven, „Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies,“ *The Computer Journal,* kd. Volume 62, pp. Pages 448-460, March 2019.

[23] F. a. Dechesne, A. M. Sears, T. Tani, S. van der Hof a ja B. Custers, „A comparison of data protection legislation and policies across the EU,“ *Computer Law & Security Review,* p. 10, December 2017.

[24] S. Barocas ja H. Nissenbaum, Big Data’s End Run around Anonymity and Consent, Cambridge University Press, 2014, pp. Pages 44-75.

[25] B.-J. Koops, „The trouble with European data protection law,“ *International Data Privacy Law,* kd. Issue 4, pp. Pages 250-261, November 2014.

[26] J. Ball, „Costeja González and a memorable fight for the 'right to be forgotten',“ *The Guardian,* 2014.

[27] B. Hammersley, „Concerned about Brexit? Why not become an e-resident of Estonia,“ *Wired,* 27 March 2017.

[28] Riigikogu, *Avaliku teabe seadus,* Tallinn: Riigiteataja, 2001.

[29] Estonia´s Information System Authority, „Data Exchange Layer X-tee,“ Estonia´s Information System Authority, 2018. [Võrgumaterjal]. Available: https://www.ria.ee/en/state-information-system/x-tee.html. [Kasutatud 2018].

[30] Riigikogu, „Infosüsteemide turvameetmete süsteem,“ Riigi Teataja, Tallinn, 2008.

[31] EISA, „RIHA - Administration system for the state information system,“ Information System Authority, 5 September 2018. [Võrgumaterjal]. Available: https://www.ria.ee/en/state-information-system/administration-system-riha.html. [Kasutatud 11 April 2019].

[32] Riigikogu, „Riigi infosüsteemi haldussüsteem,“ Riigi Teataja, Tallinn, 2008.

[33] National Audit Office of Estonia, „Implementation of system of IT security measures in local governments,“ pp. 4-7, 2018.

[34] A. C. Johnston ja M. Warkentin, „Fear Appeals and Information Security Behaviors: An Empirical Study,“ *MIS Quarterly*, pp. 549-A4, 2010.

[35] „Audits,“ Estonian Data Protection inspectorate, 2018. [Võrgumaterjal]. Available: https://www.aki.ee/et/auditid. [Kasutatud April 2019].

[36] „RIA kontrollib infoturbemeetmete rakendamist kohalikes omavalitsustes,“ Estonian Information System Authority, 2019. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/ria-kontrollib-infoturbemeetmete-rakendamist-kohalikes-omavalitsustes.html. [Kasutatud 12 April 2019].

[37] National Audit Office of Estonia, „Implementation of system of IT security measures in local governments,“ pp. 28-31, 5 June 2018.

[38] F. Häußinger, „Studies on Employees’ Information Security Awareness,“ Faculty of Economics at the Georg-August University Göttingen, Göttingen, 2015.

[39] C. J. Haug, „Turning the Tables — The New European General Data Protection Regulation,“ *The New England Journal of Medicine,* 19 July 2018.

[40] J. Abawajy , „User preference of cyber security awareness delivery methods, Behaviour & Information Technology,“ *Behaviour & Information Technology Journal,* kd. Issue 3, nr Volume 33, pp. 237-248, 2014.

[41] T. Stephanou ja R. Dagada, „The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research,“ Conference: Proceedings of the ISSA 2008 Innovative Minds Conference, 2008.

[42] J. M. Stanton, K. R. Stam, P. Mastrangelo ja J. Jolton, „Analysis of end user security behaviors,“ *Computers & Security,* pp. 1-10, July 2004.

[43] M. T. Siponen, „Five Dimensions of Information Security Awareness,“ *Computers and Society,* pp. 24-29, 2001.

[44] M. Siponen, „A conceptual foundation for organizational information security awareness.,“ *Information Management & Computer Security 8(1),* pp. pp. 31-41, 2000.

[45] P. Korovessis, S. Furnell, M. Papadaki ja P. Haskell-Dowland, „A toolkit approach to information security awareness and education,“ *Journal of Cybersecurity Education, Research and Practice,* kd. 2017, nr 2, pp. 1-34, December 2017.

[46] „Cyber Hygiene e-Learning Course,“ Cybexer Solutions, 2018. [Võrgumaterjal]. Available: https://cybexer.com/cyber-hygiene-e-learning-course/. [Kasutatud April 2019].

[47] Estonian Data Protection Inspectorate, „Andmeturve,“ Estonian Data Protection Inspectorate, 2018. [Võrgumaterjal]. Available: https://www.aki.ee/et/avalik-teave/andmeturve. [Kasutatud April 2019].

[48] L. S. Sterling, The Art of Agent-Oriented Modeling, London: The MIT Press, 2009.

[49] European Parliament and the Council of the European Union, „Principles relating to processing of personal data,“ Official Journal of the European Union, 2016.

[50] Riigikogu, „Personal Data Protection Act; Organisational, physical and information technology security measures for protection of personal data,“ Riigi Teataja, Tallinn, 2007.

Appendix 1 – Example scenarios related to the most crucial shortcomings

Sample questions and answers to the module:

CASE

The clerk of the local government receives an email and needs to register it in the information system. The email includes an evaluation of a underage child´s health. Should the document inserted in the information system have restrictions to permissions to view?

QUESTIONS

What is the correct way to register documents that include personal data?

- ☐ a. Nobody never is interested in these documents, so no need to restrict the access
- ☐ b. All documents including personal data, should be with restricted access
- ☐ c. All documents need to be hidden from the public
- ☐ d. All documents including personal data, should be restricted at least on the extent of what's considered as personal data.

ANSWER/ STUDY MATERIAL:

Every official dealing with documents including personal information, should always weigh the content of the documents before inserting the data to information systems. In order to avoid breach of data subjects rights, it is necessary to restrict the access to documents according to the law, but keeping in mind that not all data should be restricted. Additionally, when inserting documents, it is suggested to avoid typing the names of the associated data subject to the headlines.

CASE

An official received a request of concerning one of the local citizen. The documents include sensitive health information about the citizen, but the official is unsure is it sensitive data. How to determine?

QUESTIONS

What do you think, how to determine is the data belonging to special categories of data?

- [ ] a. You can decide according to your own opinion.
- [ ] b. Persons ID code
- [ ] c. Are defined in the General Data Protection regulations article 9 section 1

ANSWER/ STUDY MATERIAL:

The exhaustive list of special categories of personal data is presented in the GDPR article 9 section 1. It states that data revealing

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health or data concerning a natural person's sex life or sexual orientation

All cases, where the documents include data provided in the above sections, must be considered and handled as sensitive data.

CASE

A friend of a “A” is visiting her friend in the local government office to have a coffee break together. While having a chat, the friend is curious about a neighbours social benefits and health information. The official, has to decide whether it is correct to speak about another person’s issues, related to the information she has received in the course of her duties.

QUESTIONS

What do you think is the right way to act? When is it not allowed to issue personal data?

- [ ] a. If it can harm other people´s rights and freedoms
- [ ] b. If a person is asking his/hers spouse´s information
- [ ] c. If it can harm an criminal investigation
- [ ] d. If a person is asking data of his/her underage child
- [ ] d. If a person requiring the information has a good excuse for acquiring the information, it is okay to give it

ANSWER/ STUDY MATERIAL:

Data should be given only to the data subject or a data subject´s representative either with a valid application or when the data subject is an underage child. Data should never

be given just because someone is asking, always make sure the person who is asking has the right to inquire and receive it.

CASE

Official is asked if he/she is the data processor. The official replies that he/she only is updating existing data. Is arranging data part of data processing?

QUESTIONS

What do You think is considered as data processing?

- ☐ a. All actions with data is considered as data processing;
- ☐ b. Only deleting data is data processing;
- ☐ c. Only actions which alter the data, is considered as processing

ANSWER/ STUDY MATERIAL:

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

So even if the official is only updating the data, is already considered as data processing.

CASE

An citizen demands information/data about his/her ex-spouse. The official has to decide whether it is allowed to give the data to the citizen.

QUESTIONS

What do you think, is it alright to give an ex-spouse the information?

- ☐ a. Data should be given to a lawyer with valid application
- ☐ b. Data subject always has the right to acquire information about himself/herself
- ☐ c. a Lawyer
- ☐ d. Of course the ex-spouse should have the information, they were related with the data subject

ANSWER/ STUDY MATERIAL:

Data can only be released to the data subject or to a lawyer with a valid application, otherwise no matter how strongly the third person demands, the data should not be disclosed.

CASE

A friend of an official, knows he/she has access to an information system, which contains information that interests him/her. The friend is asking for a favour, from the official to acquire some information about a troublesome neighbour. How do you think the official should behave?

QUESTIONS

What kind of queries are allowed in the information systems?

- ☐ a. Queries about family members
- ☐ b. Queries related to work assignments
- ☐ c. Queries on behalf of a friend about a neighbour/acquaintance
- ☐ d. Queries about myself
- ☐ e. Queries about a famous politicians

ANSWER/ STUDY MATERIAL:

Officials who have access to different information systems, should avoid making inquiries out of curiosity. It in many cases, may be against the law or in most cases against policies, which should be in place. No to mention that to access data without a reason is not ethical.

CASE

A data subject is moving from one local government to another and sends the official an email, that the official should send him/her all the social benefits information which is not seen in the information systems and all the documents which are related to his/her underage childrens school evaluations. The official send the documents with plain email.

QUESTIONS

Do you think the official acted correctly? Is it necessary to encrypt documents?

- ☐ a. If the recipient does not ask for encryption, it is not necessary, it is not likely anything could happen to the documents
- ☐ b. Because encryption protects the document by making it inaccessible for individuals without the correct key, it is always good idea to encrypt;
- ☐ c. It is useful for signing the document with a digital signature
- ☐ d. Encrypting is time consuming and it is designed to make users life harder

ANSWER/ STUDY MATERIAL:

Encrypting offers the necessary safeguard in protecting the data from unauthorized access. Even if the data subject does not ask for it, the official should use encryption in order to keep the data safe. In this case, the official sent sensitive health data of a child without encrypting.

CASE

The official needs to send documents with health data to a data subject. Data subject gave the official his/her e-mail address and the official sent the documents as a plain e-mail, the documents attached.

QUESTIONS

What is the correct way to forward data subjects information:

- ☐ a. By E-mail and without encryption
- ☐ b. By E-mail and encrypted
- ☐ c. By Ordinal mail
- ☐ d. By registered mail

ANSWER/ STUDY MATERIAL:

One of easiest and very efficient way to protect documents is to encrypt them when transmitting. Even if the Data subject does not ask for it, it is always wise to use encryption.